UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
10/717,352	11/19/2003	Ramajeyam Gopalraj	LOT920030017US1	7004

23550 7590 12/18/2008

HOFFMAN WARNICK LLC
75 STATE STREET
14TH FLOOR
ALBANY, NY 12207

EXAMINER	
DAFTUAR, SAKET K	

ART UNIT	PAPER NUMBER
2451	

NOTIFICATION DATE	DELIVERY MODE
12/18/2008	ELECTRONIC

Please find below and/or attached an Office communication concerning this application or proceeding.

The time period for reply, if any, is set in the attached communication.

Notice of the Office communication was sent electronically on above-indicated "Notification Date" to the following e-mail address(es):

PTOCommunications@hoffmanwarnick.com

Office Action Summary	Application No.	Applicant(s)	
	10/717,352	GOPALRAJ, RAMAJEYAM	
	Examiner	Art Unit	
	SAKET K. DAFTUAR	2451	

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE *3* MONTH(S) OR THIRTY (30) DAYS, WHICHEVER IS LONGER, FROM THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed after SIX (6) MONTHS from the mailing date of this communication.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133). Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any earned patent term adjustment. See 37 CFR 1.704(b).

Status

1)☒ Responsive to communication(s) filed on *22 October 2008*.

2a)☒ This action is **FINAL**. 2b)☐ This action is non-final.

3)☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4)☒ Claim(s) *1-22* is/are pending in the application.

4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5)☐ Claim(s) _____ is/are allowed.

6)☒ Claim(s) *1-22* is/are rejected.

7)☐ Claim(s) _____ is/are objected to.

8)☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9)☐ The specification is objected to by the Examiner.

10)☐ The drawing(s) filed on _____ is/are: a)☐ accepted or b)☐ objected to by the Examiner.

Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11)☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12)☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

a)☐ All b)☐ Some * c)☐ None of:

1.☐ Certified copies of the priority documents have been received.

2.☐ Certified copies of the priority documents have been received in Application No. _____.

3.☐ Copies of the certified copies of the priority documents have been received in this National Stage application from the International Bureau (PCT Rule 17.2(a)).

* See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☐ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO/SB/08) Paper No(s)/Mail Date _____.
4) ☐ Interview Summary (PTO-413) Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application
6) ☐ Other: _____.

Response to Amendment

1. This office action is responsive to the amendment filed on October 22nd, 2008. Claims 1-22 are presented for the further examination.

Response to Arguments

2. Applicant's arguments filed October 22nd, 2008 have been fully considered but they are not persuasive. As per arguments filed on October 22nd, 2008, applicant argues to the substance that:

a. Gupta failed to discloses "the application data is not used for validating a session."

In response to applicant only arguments a), applicant admitted that above statement is to make it clear that application data is not used for validation purpose and argues that the application data referenced in claims would not include user ID and password for validating. It is clear from the evidence below that Gupta login server authenticate the user first before login server obtains user profile information. The login server has nothing to do with the application data as application data is processed by application server and has no concerned related to authentication (see underlined citation below). Examiner considers the evidence that Gupta discloses in column 4, line 30 – column 5, line 41, column 5, line 42- column 6, line 45 and Figure 3, column 11, line 8 – column 13, line 40.

"As an alternative to a session list, a "session service" may be utilized that is responsible for and controls access to sessions. A session service may

create, validate, and invalidate user sessions. Thus, step 304 may be performed by a session service that uses the cookies to find a session associated with the user. If there is no valid session, the application server redirects the client's request to a login server at step 306. To redirect a request, the application server sends a redirect message (with the login server's URL) back to the client's browser. The redirect message may also include the application's URL, a cookie for the application, and a temporary identifier. When a browser receives a redirect message, the browser automatically sends a request to the specified URL (e.g., the login server's URL) without any interaction from the user along with any existing cookies (or tokens) for the specified URL."

Further Gupta also discloses that "As described above, the login server checks if a request has an active and valid session, if the user has not been authenticated, the login server enforces authentication, and the login server may obtain user profile information. In this manner, the applications on the application server need not be concerned about authenticating a given user. The application server merely needs to know how to work with the login server to authenticate the user. Further, communications between the application server and login server are transparent (or without any interaction from) the user (although the user may see the browser communicating with each server)."

As argued, Gupta briefly discloses "Cookie mechanism to authenticate user on the Internet. Cookies are small pieces of information stored on individual's browsers that can later be read back from the browser. When a web site is

accessed, a cookie may be sent by the web site identifying itself to the web browser. Cookies are stored by the browser and may be read back by a server at a later date. Cookies may be utilized for a variety of reasons including the ability to personalize information, to perform targeted advertising, or to track popular links or demographics. For example, a book store on the web may store a cookie that contains the user's name and password. Thereafter, whenever the user accesses the book store's web site, the cookie is retrieved, and the user need not log in to the book store's site. Cookies can store a variety of information including database information and custom page settings. A cookie is merely an HTTP header that consists of a text-only string that gets entered into the memory of a browser. The string contains information (referred to as "parameters") such as the name of the cookie, the value of the cookie, the expiration date of the cookie, the path the cookie is valid for, the domain the cookie is valid for, and the need for a secure connection to exist to use the cookie. Each cookie has a name and value. For example, the name of a cookie may correspond to the web site owner's name (e.g., SUN_ID may be the name of the cookie for Sun Microsystems.TM.) and the value may be an identification number for the particular user. By utilizing a name and value, a web site may store personal information to be displayed to a particular user every time the cookie from that user is retrieved by the server. The expiration parameter defines the lifetime of the cookie (e.g., how long the cookie is valid for). The path parameter defines the URL path the cookie is valid for (i.e., web pages outside of the specified path

cannot read or use the cookie). The domain parameter specifies the domain that can access the cookie. For example, if the domain parameter is ".sun.com", only cookie requests that originate from pages located on the ".sun.com" domain server will be permitted. Further, after a server sends a cookie to a browser, any future requests made by the browser to the parameters specified in the cookie (e.g., the specified path and domain) the browser forwards the cookie with the request. The secure parameter is either TRUE or FALSE depending on whether a secure server condition is required to access the particular cookie.

By utilizing cookies, a server can authenticate a user based on the cookie (i.e., by reading the name and variable stored in the cookie) and not require a user to re authenticate itself each time (emphasis added). The first time a client/user accesses a server, the server may authenticate a user (e.g., using a user name and password mechanism) and issues a cookie with a name and variable that uniquely identifies the authenticated client. For example, after authenticating a user, a server may generate a unique random number, create a cookie with the unique random number as a value, and transmit the cookie back to the user's browser. The server may also store the user's information (in the server) using the unique random number as a key. Thereafter, the cookie is similar to a key in that the server merely retrieves the cookie (with the identifying information (e.g., using the unique random number as a key)) instead of requiring the user to reenter a username and password [user name and password is part of application data (emphasis added)]."

Therefore, It is clear from above citation that Gupta clearly disclose to check the session's validity and establishing a new session between applicant and client, submitting the application data without reentry of the application data by a user once the new session is ensured as valid. Therefore, applicant argument are not persuasive and the rejection is maintained.

Claim Rejections - 35 USC § 112

The following is a quotation of the second paragraph of 35 U.S.C. 112:

> The specification shall conclude with one or more claims particularly pointing out and distinctly claiming the subject matter which the applicant regards as his invention.

3. Claims 1-22 are rejected under 35 U.S.C. 112, second paragraph, as being indefinite for failing to particularly point out and distinctly claim the subject matter which applicant regards as the invention.

Claims 1-22 now recite negative limitation "the application data is not used for validating a session". It is not clear what applicant is trying to accomplish by using the negative limitation. Is applicant referring "application data" to user id and password only? or Is applicant referring "application data" to a data processed and completed by user after user gets authenticated ? There is no evidence in specification that "application data" is referred to user ID and password. Examiner has made it clear in response to arguments that user gets authenticated before and then processed the user profile information at the application server. An appropriate correction is required by applicant.

Claim Rejections - 35 USC § 101

4. 35 U.S.C. 101 reads as follows:

> Whoever invents or discovers any new and useful process, machine, manufacture, or composition of matter, or any new and useful improvement thereof, may obtain a patent therefor, subject to the conditions and requirements of this title.

5. Claims 18-22 are rejected under 35 U.S.C. 101 because the claimed invention is directed to non-statutory subject matter.

Claims 18-22 recite the limitation "computer-readable medium storing a program product for obtaining application data". Also, it appears that program product of claims 18-22 can be implemented by software only as Paragraph 42 of specification admitted that the present invention could be realized in software also and therefore, the claims lack the necessary physical articles or objects to constitute a machine or a manufacture within the meaning of 35 USC 101. They are clearly not a series of steps or acts to be a process nor are they a combination of chemical compounds to be a composition of matter. As such, they fail to fall within a statutory category. They are, at best, functional descriptive material *per se*.

Descriptive material can be characterized as either "functional descriptive material" or "nonfunctional descriptive material." Both types of "descriptive material" are nonstatutory when claimed as descriptive material *per se*, 33 F.3d at 1360, 31 USPQ2d at 1759. When functional descriptive material is recorded on some computer-readable medium, it becomes structurally and functionally interrelated to the medium and will be statutory in most cases since use of technology permits the function of the descriptive material to be realized.

Compare *In re Lowry*, 32 F.3d 1579, 1583-84, 32 USPQ2d 1031, 1035 (Fed. Cir. 1994)

Merely claiming nonfunctional descriptive material, i.e., abstract ideas stored on a computer-readable medium, in a computer, or on an electromagnetic carrier signal, does not make it statutory. See *Diehr*, 450 U.S. at 185-86, 209 USPQ at 8 (noting that the claims for an algorithm in *Benson* were unpatentable as abstract ideas because "[t]he sole practical application of the algorithm was in connection with the programming of a general purpose computer.").

Claim Rejections - 35 USC § 102

6. The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

7. Claims 1- 22 are rejected under 35 U.S.C. 102(b) as being anticipated by Gupta et al. U.S. Patent Number 6,226,752 B1 (hereinafter Gupta).

As per claim 1, Gupta discloses obtaining a data page from a network application during a session of a client (see column 2, lines 15- 67, Figure 3); receiving an original submission of the application data using the data page (see column 2, lines 15- 67, Figure 3), wherein the application data is not used for validating a session (see column 4, line 30 – column 5, line 41, column 5, line 42- column 6, line 45 and Figure 3, column 11, line 8 – column 13, line 40, examiner

considers if the user has not been authenticated, the login server enforces authentication, and the login server may obtain user profile information, also see response to the argument) ; ensuring that the session is valid (see column 4, line 30 - column 5, line 41; Figure 3); and submitting the application data to the network application when the session is valid (see column 4, line 30 - column 5, line 41; Figure 3) wherein when the session is invalid and a new session between applicant and client is established the application data is submitted to the network application without reentry of the application data by a user once the new session is ensured as valid (see column 4, line 30 – column 5, line 41, column 5, line 42- column 6, line 45 and Figure 3, column 11, line 8 – column 13, line 40, using cookies to submit user data to authenticate a user and not require a user to re authenticate itself as user name and variable are stored in the cookie).

As per claim 2, Gupta discloses establishing the session of a client with the network application (see column 4, line 30 - column 5, line 41; Figure 3).

As per claim 3, Gupta discloses receiving a submission request for the application data (see column 4, line 30 - column 5, line 41; Figure 3).

As per claim 4, Gupta discloses determining if it is probable based upon a measure of session inactivity that the session may have expired (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; Figure 4); and querying the network application for a session status if it is probable based upon a measure of

session inactivity that the session has expired (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; Figure 4).

As per claim 5, Gupta discloses sending a request to the network application (see column 4, line 30 - column 5, line 41; Figure 3); and determining whether a login page is received from the network application in response to the request (see column 4, line 30 - column 5, line 41; Figure 3).

As per claim 6, Gupta discloses obtaining a session time remaining at a first time (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 11, line 45 – column 12, line 6; Figures 3- 4); determining a submission time for the submission request (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 11, line 45 – column 12, line 6; Figures 3- 4); and comparing the session time remaining to a difference between the submission time and the first time (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 11, line 45 – column 12, line 6; Figures 3- 4).

As per claim 7, Gupta discloses the first time comprises a display time for the data page (column 11, line 45 – column 12, line 6; Figures 3- 4).

As per claim 8, Gupta discloses the ensuring step comprises establishing another session of a client with the network application if the session is invalid (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 12, lines 14-24; Figures 3- 4).

As per claim 9, Gupta discloses data page is displayed in a first window, and wherein the establishing step includes displaying a login page in a second

window (See abstract, see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 11, line 45 – column 12, line 6; Figures 3- 4, application server redirects the user to login server and when authenticated login server redirects the user back to the application server inherently discloses data page is displayed in a first window, and wherein the establishing step includes displaying a login page in a second window).

As per claim 10, Gupta discloses establishing a session of a client with the network application (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3); providing a data page to the client, wherein the data page ensures that the session is valid before submitting the application data (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3); and receiving an original submission of the application data from the client (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3), wherein when the session is invalid and a new session between applicant and client is established the application data is submitted to the network application without reentry of the application data by a user once the new session is ensured as valid (see column 4, line 30 – column 5, line 41, column 5, line 42- column 6, line 45 and Figure 3, column 11, line 8 – column 13, line 40, using cookies to submit user data to authenticate a user and not require a user to re authenticate itself as user name and variable are stored in the cookie).

As per claim 11, Gupta discloses providing a login page to the client (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3); receiving

login data from the client (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3); and authenticating the login data (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3).

As per claim 12, Gupta discloses receiving a request from the client for an invalid session (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; column 11, line 45 – column 12, line 24; Figure 3 - 4); and providing the login page to the client in response (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; column 11, line 45 – column 12, line 24; Figure 3 - 4).

As per claim 13, Gupta discloses the data page includes a session time remaining (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; column 11, line 45 – column 12, line 6; Figure 3 - 4).

As per claim 14, Gupta discloses determining a display time for the data page (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 11, line 45 – column 12, line 6; Figures 3- 4); determining a submission time for a submission request (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 11, line 45 – column 12, line 6; Figures 3- 4); and comparing the session time remaining to a difference between the submission time and the first time (see column 5, line 42 - column 6, line 51; column 7, lines 1-15; column 11, line 45 – column 12, line 6; Figures 3- 4).

As per claim 15, Gupta discloses a session system for establishing a session of a client with the network application (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3); and a data system for providing a

data page to the client and receiving an original submission of the application data from the client (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3); wherein the data page ensures that the session is valid before submitting the application data (see column 2, lines 15- 67, column 4, line 30 - column 5, line 41; Figure 3) and wherein when the session is invalid and a new session between applicant and client is established the application data is submitted to the network application without reentry of the application data by a user once the new session is ensured as valid (see column 4, line 30 – column 5, line 41, column 5, line 42- column 6, line 45 and Figure 3, column 11, line 8 – column 13, line 40, using cookies to submit user data to authenticate a user and not require a user to re authenticate itself as user name and variable are stored in the cookie).

As per claim 16, Gupta discloses the system of claim 15, further comprising a display system for displaying pages to a user (see column 5, line 42 - column 6, line 51).

As per claim 17, Gupta discloses the system of claim 15, wherein the session system provides a login page to the client in response to a request for an invalid session (see column 4, line 30 - column 5, line 41; column 11, line 45 – column 12, line 24; Figure 3 - 4).

As per claims 18-22, claims 18-22 are program product claims of method claims of 1-3, 5-6 and 9. They do not teach or further define over the limitation as

recited in claims 1-3, 5-6 and 9. Therefore, claims 18-22 are rejected under same scope as discussed in claims 1-3, 5-6 and 9, supra.

Conclusion

8. **THIS ACTION IS MADE FINAL.** Applicant is reminded of the extension of time policy as set forth in 37 CFR 1.136(a).

A shortened statutory period for reply to this final action is set to expire THREE MONTHS from the mailing date of this action. In the event a first reply is filed within TWO MONTHS of the mailing date of this final action and the advisory action is not mailed until after the end of the THREE-MONTH shortened statutory period, then the shortened statutory period will expire on the date the advisory action is mailed, and any extension fee pursuant to 37 CFR 1.136(a) will be calculated from the mailing date of the advisory action. In no event, however, will the statutory period for reply expire later than SIX MONTHS from the mailing date of this final action.

Contact Information

9. Any inquiry concerning this communication or earlier communications from the examiner should be directed to SAKET K. DAFTUAR whose telephone number is (571)272-8363. The examiner can normally be reached on 7:00 - 3:30pm M-W.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, John Follansbee can be reached on 571-272-3964. The fax phone number for the organization where this application or proceeding is assigned is 571-273-8300.

Information regarding the status of an application may be obtained from the Patent Application Information Retrieval (PAIR) system. Status information for published applications may be obtained from either Private PAIR or Public PAIR. Status information for unpublished applications is available through Private PAIR only. For more information about the PAIR system, see http://pair-direct.uspto.gov. Should you have questions on access to the Private PAIR system, contact the Electronic Business Center (EBC) at 866-217-9197 (toll-free). If you would like assistance from a USPTO Customer Service Representative or access to the automated information system, call 800-786-9199 (IN USA OR CANADA) or 571-272-1000.

/S. K. D./
Examiner, Art Unit 2451

/John Follansbee/

Supervisory Patent Examiner, Art Unit 2451